UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

MARITZ HOLDINGS INC.,	)	
	)	
Plaintiff,	)	
	)	
v.	)	Case No. 4:18-cv-00826
	)	
COGNIZANT TECHNOLOGY SOLUTIONS U.S. CORPORATION,	)	
	)	
	)	
Defendant.	)	

PLAINTIFF'S MEMORANDUM IN OPPOSITION TO DEFENDANT'S MOTION TO DISMISS

THOMPSON COBURN LLP

Jan Paul Miller, 58112MO
Brian A. Lamping, 61054MO
Kristen E. Sanocki, 67375MO
One US Bank Plaza
St. Louis, Missouri 63101
314-552-6000
FAX 314-552-7000
jmiller@thompsoncoburn.com
blamping@thompsoncoburn.com
ksanocki@thompsoncoburn.com

Attorneys for Plaintiff Maritz Holding, Inc.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Constitutional Provisions

Rules

INTRODUCTION

The Court should deny Defendant Cognizant Technology Solutions U.S. Corporation's ("Cognizant") Motion to Dismiss (Dkt. No. 15). Cognizant flouts Rule 8(a)(2) and Supreme Court precedent when it criticizes Plaintiff Maritz Holdings, Inc. ("Maritz") for failing to attach "forensic evidence" tying Cognizant to the massive cyber-attacks that decimated Maritz in 2016 and 2017. Maritz need provide only a "short and plain statement of the facts entitling it to relief," Fed. R. Civ. P. 8(a)(2); Maritz need only plead sufficient facts to create a reasonable inference that Cognizant either hacked Maritz' system or negligently allowed someone to hack the system. Here, Maritz has alleged that Cognizant employees used Cognizant accounts to hack Maritz' computer system in 2017; Maritz has alleged that Cognizant employees improperly shared credentials and passwords for Cognizant accounts, at least one of which was used to hack Maritz' system; and Maritz has alleged facts connecting the 2017 attack to the larger attack in 2016. Maritz has therefore pled sufficient facts to state the claims asserted in the Complaint.

BACKGROUND

Maritz will not repeat the facts asserted by Cognizant in its Background section about the parties' relationship – their agreement speaks for itself. Maritz will instead focus on the facts that Cognizant has ignored, which create a reasonable inference that the Cognizant employees who attacked Maritz' system in 2017 were responsible for—or at the very least involved with—the persons who attacked Maritz' system in 2016.

In March 2016, Maritz learned that participants in one of its customer's eGift Card programs received eGift Cards with no value. Compl. at ¶ 26. Maritz reported the issue to a data security firm, Charles River Associates ("CRA"). Compl. at ¶ 27. CRA discovered the following:

- In March 2016, over 200 Maritz employees received phishing emails from unknown perpetrators (Compl. at ¶ 28);
- These emails contained a malicious file in an attached Microsoft Word document (*id*.);
- The phishing emails infected several computers on the Maritz system with a "backdoor" and other malware (*id.)*; and
- The perpetrators obtained access to Maritz' L-Drive, where Maritz stores its eGift Cards, and transferred 1.2 gigabytes of data from the Maritz server (*id.*).

The 2016 attack caused Maritz over $11 million in damages (*id.* at ¶¶ 31-36).

Maritz was attacked a second time in 2017. It hired Intersec Worldwide ("Intersec") to investigate. Intersec discovered that the 2017 attackers, like the 2016 attackers, initiated the attack by sending to Maritz employees phishing emails that installed a malicious file (remote access tools) on the Maritz system. *Id*. at ¶ 39. Intersec discovered that the 2017 attackers, like the 2016 attackers, used a program called Screen Connect to carry out the attack. *Id*. at ¶ 42. Intersec also learned that 2017 attackers ran searches on the Maritz system for certain words and phrases connected to the 2016 attack. *Id*.[1] Finally, Intersec learned that the 2017 attackers used accounts registered to Cognizant employees who worked on the Maritz account. *Id*. at ¶ 43.

Thus, Maritz has direct evidence that Cognizant employees were responsible for the 2017 attack (use of Cognizant accounts) and strong circumstantial evidence that the same people who controlled those Cognizant accounts were also responsible for the 2016 attack (use of Screen Connect and knowledge of information about the 2016 attack). These and other facts create a reasonable inference that Cognizant employees hacked Maritz' computer system and are responsible for over $12 million in losses sustained by Maritz from the attacks.

[1] The hackers ran these searches to determine whether Maritz had contacted the authorities about the 2016 attack and whether Maritz knew that the attackers used Screen Connect.

ARGUMENT

I. Legal Standard.

A well-pleaded complaint requires only "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). "Specific facts are not necessary; the statement need only 'give the defendant fair notice of what the . . . claim is and the grounds upon which it rests." *Erickson v. Pardus*, 551 U.S. 89, 93 (2007) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007)). When ruling on a motion to dismiss, "a court must accept as true all of the factual allegations contained in the complaint." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). A court must "draw all reasonable inferences in favor of the nonmoving party." *Coons v. Mineta*, 410 F.3d 1036, 1039 (8th Cir. 2005).

II. Maritz Pled Sufficient Facts for the Court to Infer That One or More Cognizant Employees Attacked Maritz' Computer System in 2016.

Cognizant (at 4) erroneously claims that Maritz failed to allege facts connecting Cognizant to the 2016 attack and, therefore, the Court should "disregard" those allegations. To the contrary, Maritz alleges that, in 2017, one or more Cognizant employees used Cognizant accounts to steal over $1.2 million from Maritz' system. Compl. at ¶¶ 39, 43. Maritz alleges that the 2017 attackers used the same program to access Maritz' computers (Screen Connect) as the 2016 attackers. Compl. at ¶¶ 42-43. Although the use of Screen Connect—standing alone—may be insufficient to connect the 2016 and 2017 attacks, Maritz has also alleged that the 2017 attackers "had run searches on the Maritz system for certain words and phrases connected to the Spring 2016 attack." Compl. at ¶ 42. If the 2017 attackers were aware of words and phrases connected to the 2016 attack and used the same computer program as the 2016 hackers, the Court can reasonably infer that they were also involved in the 2016 attack. *Coons*, 410 F.3d at

1039 (court must "draw all reasonable inferences in favor of the nonmoving party"). The Court should not disregard the 2016 allegations.

III. The Court Should Not Dismiss Maritz' Claims Under the CFAA or MCTS Because Maritz has Pled Facts to Show That One or More Cognizant Employees Intentionally and Knowingly Hacked Maritz' System.

Cognizant argues (at Section II.A.) that the Court should dismiss Maritz' claims under the

Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2) ("CFAA") and Missouri's computer tampering statutes, Mo. Rev. Stat. § 537.525, 569.095 ("MCTS"), because Maritz has failed to allege that any Cognizant employee intentionally or knowingly hacked into Maritz' computer system.[2] According to Cognizant (at 6), because both the 2016 and 2017 attacks utilized phishing emails associated with Cognizant accounts, a Cognizant employee could not have been involved because phishing emails, "by definition," are sent by third parties who are not associated with the person/company that sent the phishing email.

But Maritz ***does not*** allege that the phishing emails originated from a Cognizant account. Rather, Maritz alleges that the phishing emails (sent from an "unidentified perpetrator," Compl. at ¶ 28.a.) were successful in loading malicious files within the Maritz computer system. Compl. at ¶¶ 28, 39. One or more Cognizant employees then used their Cognizant accounts to enter the Maritz system and used the malicious files to obtain broad access to Maritz' computer system, allowing them to steal redemption codes. Compl. at ¶¶ 39, 42-43. It is reasonable to infer that whoever used the Cognizant accounts to steal from Maritz in 2017 would not have known about the malicious files unless they were involved with the phishing attacks. *Coons*, 410 F.3d at 1036.

[2] Cognizant does not claim that Maritz has failed to establish any of the other elements of its claims under the CFAA and MCTS.

Citing *Thomas v. Zion Lutheran Sch.*, No. 4:12CV2243 JCH, 2012 WL 6093704 (E.D. Mo. Dec. 7, 2012), Cognizant characterizes Maritz' theory as "conclusory." In *Thomas*, the plaintiff alleged that the defendant had an "evil motive" without supporting that legal conclusion with a shred of factual support. Here, however, Maritz has alleged that Cognizant employees ***using accounts assigned to Cognizant*** stole millions from its computer system, and that these same attackers did so by relying on malicious files that were loaded onto Maritz' system through the successful phishing attacks. Compl. at ¶¶ 39, 43. Maritz has also alleged facts connecting the 2017 attack to the 2016 attack, as described above. Although Cognizant speculates that an unknown third party (rather than Cognizant employees) used the Cognizant accounts to steal from Maritz, Cognizant's theory is inconsistent with the facts alleged in the Complaint, and the Court must accept Maritz' theory at this stage. *Starr v. Baca*, 652 F.3d 1202, 1216 (9th Cir. 2011) ("If there are two alternative explanations, one advanced by defendant and the other advanced by plaintiff, both of which are plausible, plaintiff's complaint survives a motion to dismiss under Rule 12(b)(6). Plaintiff's complaint may be dismissed only when defendant's plausible alternative explanation is so convincing that plaintiff's explanation is implausible.").[3]

IV. Maritz Has Pled Sufficient Facts to State a Claim Under the CFAA and MCTS.

According to Cognizant, Maritz was required to plead that Cognizant "urged" or "induced" the attacks to state claims under the CFAA and MCTS based on vicarious liability. Although several courts have applied this heightened pleading standard for CFAA claims alleging vicarious liability, the Eighth Circuit does not appear to have taken a position on this

[3] Cognizant's argument that the "success of the phishing attacks" makes it "likely that any account compromise resulted from those attacks, not from accounts being used by authorized users" is non-sensical. The phishing attacks uploaded malicious files onto the Maritz system. Without more, Maritz would have suffered no damages. But persons using Cognizant accounts later used those malicious files to steal from Maritz. Thus, Cognizant's "chicken and the egg" argument is without merit.

issue, and at least one other court has allowed discovery to proceed on a CFAA claim against an employer without imposing this heightened showing. *See Physicians Interactive v. Lathian Sys., Inc.*, No. CA 03-1193-A, 2003 WL 23018270, at *9 (E.D. Va. Dec. 5, 2003) (citing cases applying general principles of respondent superior from Restatement (Second) of Agency, § 219). Here, as set forth in more detail below and in Section V, Maritz has alleged sufficient facts to state a claim against Cognizant under general respondeat superior principles.

Cognizant, however, cites no authority for its assumption that the heightened standard also applies to claims under the MCTS. Although no Missouri court appears to have confronted this precise issue, the decision in *U.S. Bancorp Investments, Inc. v. Signature Bank, Inc.*, No. 05-3418-CV-S-RED, 2007 WL 9718117 (W.D. Mo. July 24, 2007) is instructive. There, the plaintiff asserted a claim under the MCTS against several of its former employees and their new employer, Signature Bank, after the former employees removed confidential information from the plaintiff's files before they resigned. *Id.* at *2. In analyzing whether the plaintiff could hold Signature Bank vicariously liable under the MCTS for the former employees' actions, the court did not impose a heightened standard for establishing vicarious liability. *Id.* at *7. Rather, the court looked to the general rule on vicarious liability in Missouri: "an employer is vicariously liable for the misconduct of an employee or agent acting within the course and scope of employment agency." *Id*. (citing *McHaffie v. Bunch*, 891 S.W.2d, 822, 825 (Mo. banc 1995)).

Here, Cognizant employees who work on the Maritz account have special accounts that allow them to access the Maritz computer system. Maritz has alleged that one or more Cognizant employees, while acting in the scope of their employment and under the control and supervision of Cognizant, intentionally accessed Maritz' network using those accounts and removed confidential information belonging to Maritz, including codes and data for Gift Cards. Compl.

¶50. Under Missouri law, Maritz has pled sufficient facts to hold Cognizant vicariously liable for those actions.

V. Maritz States a Cognizable Claim for Conversion.

The well-pleaded allegations in the Complaint establish a plausible claim for conversion. The Complaint alleges that Cognizant's employees, while acting in the scope of employment, took possession of Maritz' codes and data without authorization, thereby misappropriating them. Compl. ¶ 60. The Complaint also alleges that Cognizant's employees intentionally accessed Maritz' network and removed information belonging to Maritz (including, but not limited to, codes and data for Gift Cards and/or eGift Cards) without authorization and while using the same Cognizant accounts they used when performing services for Maritz. *Id.* at ¶ 50 (incorporated into Count III - Conversion). Maritz therefore states a claim for conversion.[4] *Goodland Foods, Inc. v. Waddell, Inc.*, No. 4:16 CV 31 JMB, 2016 WL 1060374, at *3 (E.D. Mo. Mar. 17, 2016) (stating elements of conversion under Missouri law).

Cognizant argues (at 9) that it cannot be held vicariously liable for conversion because the alleged acts did not occur within the scope of employment. Essentially, Cognizant seeks a premature ruling at the pleading stage that it is not liable for conversion.

Under the doctrine of respondeat superior, an employer can be liable for torts of its employees "even if the employer did not authorize the employee's conduct." *Daugherty v. Allee's Sports Bar & Grill*, 260 S.W.3d 869, 872 (Mo. App. W.D. 2008). "As long as the employee committed such act while engaged in an activity falling within the scope of the

[4] Cognizant argues (at 9) that Maritz' conversion claim fails because it does not include allegations of "specific intent" to take Maritz' property. Cognizant, however, misstates the intent standard for a conversion claim. To establish a conversion claim, "it is not essential to prove that the defendant acted with wrongful motive or intent." *Moore Equip. Co. v. Callen Const. Co.*, 299 S.W.3d 678, 682 (Mo. App. W.D. 2009). The factual allegations under Count III more than satisfy the intent standard articulated in *Moore*.

employee's authority or employment," the employer can be held liable. *Id*. Acts within the "course and scope of employment" are those that are (1) "done to further the business or interests of the employer under his general authority and direction" or those (2) "which naturally arise from the performance of the employer's work." *Id.* at 872-873.

Maritz' conversion claim is based on the conduct of Cognizant's employees "acting in the scope of their employment." Compl. ¶ 60. The Complaint contains several factual allegations supporting that the conduct causing the conversion naturally arose from the employee's work. *See Daugherty*, 260 S.W. 3d at 873 ("naturally, implies that the employees' conduct must be usual, customary and expected.") For example, Maritz alleges that the cyberattack occurred "under supervision of Cognizant" and by "someone using a Cognizant account [who] utilized the 'fiddler' hacking program to circumvent cyber protections that Maritz had installed." *Id.* at ¶¶ 43, 60. Maritz alleges that "Cognizant employees violated industry standards and Maritz company policy by sharing credentials and usernames for Cognizant accounts" which were "used to hack the Maritz system" and take the Gift Cards and/or eGift Cards. *Id.* at ¶¶ 44, 45.

These facts and the reasonable inferences therefrom establish that Cognizant employees committed a tort (conversion of Gift Cards and/or eGift Cards) while engaging in an activity that was usual, customary and expected (performing services under the Agreement). *See Daugherty*, 260 S.W. 3d at 873. The claim is therefore not subject to dismissal.

VI. Maritz Sufficiently Alleges a Claim for Breach of the Master Services Agreement.

The factual allegations in the Complaint establish each and every element of a breach of contract claim: (1) the parties entered into the Agreement, a valid and enforceable contract, (2) the rights of Maritz and the obligation of Cognizant under the Agreement, (3) Cognizant's four

separate breaches of obligations under the Agreement, and (4) damages resulting to the Maritz from the breach. Compl. ¶¶ 61-70; *Compass Bank v. Eager Rd. Assocs., LLC*, 922 F. Supp. 2d 818, 823 (E.D. Mo. 2013) (stating elements of breach of contract claim). Cognizant fails to identify a legitimate deficiency in Maritz' breach of contract claim.

A. Maritz states a breach of contract claim because Cognizant failed to prevent its employees from accessing Maritz' computer data for improper purposes.

Cognizant is correct that the precise phrase "prevent Cognizant employees or other unauthorized personnel from accessing Maritz' systems for improper purposes" does not appear in the text of the Agreement. That does not mean, however, that Cognizant's failure does not constitute a breach of the Agreement.

When Cognizant and Maritz entered into the Agreement, Cognizant made several promises. Cognizant "assume[d] responsibility for the services that it performed for Maritz" (Compl. ¶¶ 12, 62; Ex. 1); it promised it would "perform the services in accordance with the highest industry standards of workmanship and professionalism" (*id.* at ¶¶ 13, 62; Ex. 1); it promised to "safeguard Maritz' confidential and proprietary information (*id.* at ¶¶ 17, 62; Ex. 1); and it promised to supply only "qualified and experienced" personnel who would perform work "in compliance with applicable laws, rules and regulations" (*id.* at ¶¶ 17, 63; Ex. 1).

The allegations in the Complaint plausibly establish that Cognizant breached each of these obligations when it failed to prevent its employees or other unauthorized personnel from accessing Maritz' systems for improper purposes (i.e., taking codes and data for gift cards and eGift cards). Compl. ¶ 43-45, 50, 64. *See Twombly*, 550 U.S. at 555.

B. Maritz states a cognizable claim that Cognizant breached the Agreement by failing to prevent its employees from sharing credentials and usernames.

The Complaint alleges that Cognizant breached the Agreement's confidentiality provisions by failing to prevent its employees from inappropriately sharing credentials and account information. Compl. ¶¶ 17, 44-45, 62. This shared information was used to hack the Maritz system in 2017. *Id.* Notwithstanding these very straightforward allegations, Cognizant argues that this claim fails because the Agreement does not prohibit such sharing *among* Cognizant's employees. Cognizant's argument is flawed because it ignores that the Agreement also restricts the use of confidential information "for any purpose" outside of the Agreement. Ex. 1, p. 20. Indeed, Cognizant agreed "it would safeguard Maritz' confidential and proprietary information." Compl. ¶¶ 17, 62; Ex.1. The Agreement, attached to the Complaint, likewise states that neither party shall "use the Confidential Information of the other Party for any purpose whatsoever except as expressly contemplated under this Agreement…" Ex. 1, p. 20. Together, these allegations show that Cognizant employees' inappropriate use and sharing of confidential information for Cognizant accounts—even internally—violated the confidentiality provision of the Agreement, particularly when at least one of the accounts at issue was used to hack Maritz' system.

Cognizant's argument that the Complaint does not allege damages stemming from the breach likewise fails.[5] The Complaint specifically pleads that these actions "caused Maritz to suffer damages." Compl. ¶ 65. Even more, the Complaint links the credential sharing to the

[5] Even if the Complaint did not factually link the alleged breach to the asserted damages (it does), that is not fatal to Maritz' claim. To plead a claim for breach of contract, "a plaintiff need only plead facts sufficient to demonstrate the existence of a valid contract and its breach." *Monsanto Co. v. Omega Farm Supply, Inc.*, 91 F. Supp. 3d 1132, 1137 (E.D. Mo. 2015). This is because factual allegations that establish a valid contract and a breach are sufficient to state a claim for at least nominal damages. *Shirley's Realty, Inc. v. Hunt*, 160 S.W.3d 804, 808 (Mo. App. W.D. 2005) ("Nominal damages are available upon proof of the contract and its breach, regardless of whether actual damages have been proven."). Thus, Maritz has established a breach of the confidentiality provision.

attack. *See* Compl. ¶ 45 ("At least one of these accounts as to which Cognizant employees shared credentials and usernames was used to hack the Maritz system in 2017.")

C. The Complaint states a claim for breach of Cognizant's contractual duty to take responsibility for security breaches.

Cognizant's contention that Maritz had no obligation to take responsibility for both actual and potential security breaches (and therefore committed no breach) is baseless. Paragraph 16 of the Complaint quotes Section 6.2.2 of the Agreement, which provides "Cognizant 'shall be responsible for and shall immediately notify Maritz of, investigate and remedy any security breaches or potential security breaches…'". Compl. ¶ 16; Ex. 1 (p. 13). Under the Agreement and as pleaded, Cognizant had a duty to take responsibility for security breaches. Cognizant otherwise makes no claim that the factual allegations giving rise to this breach are deficient. Therefore, Cognizant's motion on this point should be denied.

D. Maritz states a claim for breach of the Agreement based on Cognizant's inappropriate billing of service time spent engaging in cyberattacks.

Count IV alleges that Cognizant (1) breached the Agreement by (2) billing Maritz for service time provided by the employees involved in accessing Maritz' computer systems for improper purposes, including efforts to attack Maritz' systems, and (3) as a result, suffered damages. Compl. ¶¶ 66-70. Count IV likewise identifies the provisions under which Maritz claims a breach. *Id.* at ¶¶ 12, 62; Ex. 1 (Cognizant agreed it would "assume responsibility for the services that it performed for Maritz"); *Id.* at ¶¶ 13, 62; Ex. 1 (Cognizant agreed it would "perform the services in accordance with the highest industry standards of workmanship and professionalism"); *Id.* at ¶¶ 15, 63; Ex. 1 (Cognizant agreed it would supply only "qualified and experienced" personnel who would perform work "in compliance with applicable laws, rules and

regulations"). These allegations establish a claim for breach of contract under Missouri law and meet the notice pleading requirements of Federal Rule of Civil Procedure 8(a).

Despite these lengthy allegations, Cognizant contends (at 13) the Complaint is "utterly devoid of detail" because it does not include employee names, any relevant Statements of Work, and the amount of time billed. Maritz, however, is not required to establish that level of detail. *See Iqbal*, 556 U.S. at 678 ("the pleading standard Rule 8 announces does not require detailed factual allegations…"); *Myers v. KNS Dev. Corp.*, No. 2:17-CV-04076-NKL, 2017 WL 4202242, at *3 (W.D. Mo. Sept. 21, 2017) ("Unlike claims of fraud or mistake, however, claims for breach of contract are not subject to a heightened pleading standard.")[6]

VII. Maritz Adequately Alleges a Claim for Negligence.

A plaintiff states a cause of action for negligence when it alleges that: (1) a duty exists; (2) the duty was breached; (3) proximate causation; and (4) actual damages. *Howard v. Frost Nat'l Bank*, 458 S.W.3d 849, 853 (Mo. App. E.D. 2015). Cognizant challenges only the first element, claiming that Maritz has failed to identify any tort duties that apply to the conduct alleged in the Complaint. The Court should reject this argument for two reasons.

First, Maritz has pled facts establishing that Cognizant breached its duty to exercise due care in the performance of its obligations under the Agreement. Although "[a] mere failure to complete the undertaking required by contract does not give rise to a cause of action in tort . . . the failure to exercise due care in the performance of contract undertakings" can give rise to a

[6] The remainder of Cognizant's arguments—whether Cognizant's employees contributed to the cyberattack and the extent to which Cognizant billed Maritz for improper purposes—go to the merits of the claim and are not properly assessed under Cognizant's motion. *Tower Vill., Inc. v. Serv. Employees Int'l Union, AFL-CIO, CLC Local 2000*, 377 F. Supp. 2d 733, 737 n. 5 (E.D. Mo. 2005) ("[I]n the context of a Motion to Dismiss, the Court merely reviews the Complaint to determine whether Plaintiff has stated a claim for relief; the Court does not reach the merits of the dispute."). Maritz has adequately alleged facts establishing that Cognizant employees engaged in cyberattacks, took Gift Cards and/or eGift Cards, and inappropriately billed Maritz for purported work that included wrongdoing. Compl. ¶¶ 43-45, 50-51, 59-60, 64, 66-68.

negligence. *Preferred Physicians Mut. Mgmt. Grp. v. Preferred Physicians Mut. Risk Retention*, 918 S.W.2d 805, 814 (Mo. App. W.D. 1996) (citation omitted). Here, Cognizant entered into a contract requiring it to "provide technical expertise" in connection with various Maritz projects (applications), among other obligations. To perform its contractual obligations, Cognizant employees had accounts that allowed them to obtain access to Maritz' system. Maritz has alleged that Cognizant employees shared credentials and usernames for these accounts, and that at least one of these accounts was used to hack the Maritz system in 2017. Maritz has alleged that Cognizant violated industry standards and Maritz company policy. Maritz has therefore alleged sufficient facts to state a claim for negligence.

Second, Maritz has pled sufficient facts to establish that Cognizant breached its duty to prevent foreseeable harm. Cognizant has a duty to exercise reasonable care when its conduct creates a foreseeable risk of injury to others. *Cupp v. National Railroad*, 138 S.W.3d 766, 772 (Mo. App. E.D. 2004). As stated above, Cognizant employees have accounts allowing them to access Maritz' computer system, where Maritz stores millions of dollars' worth of confidential information, including eGift Card codes. Failing to safeguard the passwords and credentials for those accounts creates a foreseeable risk that the accounts could become compromised by a third party, as Cognizant claims (at 6). Although Cognizant claims "there is no general tort duty to protect another's computer network, nor is there a general duty to safeguard login credentials," such duties exist where, as here, a reasonable person would know that sharing passwords and credentials to a computer system creates a risk of hacking. *Berga v. Archway Kitchen & Bath, Inc.*, 926 S.W.2d 476, 479 (Mo. App. E.D. 1996) ("The duty owed is generally measured by whether or not a reasonably prudent person would have anticipated danger and provided against it.")

Finally, Cognizant claims that Maritz' negligence claim is duplicative of its breach of contract claim. This argument is particularly disingenuous given that Cognizant claims (at 11) that no contractual provision requires Cognizant to "prevent Cognizant employees or other unauthorized personnel from accessing Maritz' []system for improper purposes" and that the Agreement does not preclude Cognizant employees from sharing credentials (at 12). Nevertheless, simply because Maritz and Cognizant have a contract does not foreclose negligence claims related to the performance of the contract. If Cognizant fails to take reasonable precautions in performing its contractual duties (e.g., sharing passwords and usernames), and that failure causes harm to Maritz (as it did here), the remedy lies in tort. *Preferred Physicians*, 918 S.W.2d 805.[7]

VIII. Maritz Adequately Alleges a Claim for Unjust Enrichment.

In Count VI,[8] Maritz alleges the elements of an unjust enrichment claim: (1) Maritz conferred a benefit on Cognizant by paying for purportedly appropriate work on its matter; (2) Cognizant accepted and retained the benefit of the payment; and (3) acceptance of that benefit was inequitable given that Cognizant received payment for time spent engaged in wrongdoing. Compl. ¶¶ 76-79; *Simply Thick, LLC v. Thermo Pac, LLC*, No. 4:13-CV-1036 CAS, 2014 WL 4802035, at *4 (E.D. Mo. Sept. 23, 2014) (stating the elements of unjust enrichment under Missouri law). For that reason alone, Maritz' unjust enrichment claim cannot be dismissed at the pleading stage.

[7] The time for determining whether Maritz' claims are duplicative or inconsistent with its breach of contract claim is before the case goes to the jury, viewed in light of the evidence obtained through discovery. Asserting alternative or inconsistent claims at this stage is proper and permissible. Fed. R. Civ. P. 8(d)(2).

[8] Cognizant argues that Maritz has not pleaded a claim for accounting. To the contrary, the facts in the Complaint and the reasonable inferences therefrom establish the elements of an accounting: (1) the need for discovery (¶ 81); (2) the complicated nature of the accounts due to the fact the Cognizant billed for services that included its employees' efforts to attack Maritz' systems (¶¶ 68,77); (3) the existence of a relationship of trust (¶¶ 10-11); and (4) inadequacy of legal remedies (¶ 80). *See Cook v. Martin*, 71 S.W.3d 677, 680–81 (Mo. App. W.D. 2002) (stating the elements of an accounting claim).

Cognizant appears to argue that the unjust enrichment claim is barred because Maritz is limited to recovery on the Agreement. Cognizant, however, may not simultaneously (1) argue that the contract provides no relief for Maritz *and* (2) argue that the contract claims bar other means of recovery. Maritz is entitled to plead and pursue alternate theories at this stage. *See* Fed. R. Civ. P. 8(d) ("[a] party may set out two or more statements of a claim or defense alternatively or hypothetically…"); *Chem Gro of Houghton, Inc. v. Lewis Cty. Rural Elec. Co-op. Ass'n*, No. 2:11CV93 JCH, 2012 WL 1025001, at *3 (E.D. Mo. Mar. 26, 2012) ("Plaintiff is permitted to plead both claims.") This is true even if Maritz' unjust enrichment claim incorporates its breach of contract allegations. *Collins v. Veolia ES Indus. Servs., Inc.*, No. 4:15-CV-00743-AGF, 2015 WL 8663994, at *5 (E.D. Mo. Dec. 14, 2015) ("plaintiffs are permitted to plead [breach of contract and unjust enrichment]…regardless of consistency").

CONCLUSION

For the foregoing reasons, Maritz Holdings, Inc. respectfully requests the Court deny Cognizant Technology Solutions U.S. Corporation's Motion to Dismiss in its entirety.

Respectfully submitted,

THOMPSON COBURN LLP

By: */s/ Jan Paul Miller*

Jan Paul Miller, 58112MO
Brian A. Lamping, 61054MO
Kristen E. Sanocki, 67375MO
One US Bank Plaza
St. Louis, Missouri 63101
314-552-6000
FAX 314-552-7000
jmiller@thompsoncoburn.com
blamping@thompsoncoburn.com
ksanocki@thompsoncoburn.com

Attorneys for Plaintiff Maritz Holding, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on October 2, 2018, the foregoing was filed electronically with the Clerk of Court to be served by operation of the Court's electronic filing system to all counsel of record.

/s/ Jan Paul Miller